

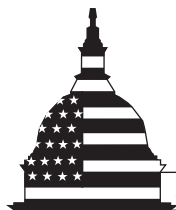
GAO

Report to the Committee on Commerce,
Science, and Transportation,
U.S. Senate

May 2011

GENERAL AVIATION

Security Assessments at Selected Airports



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-11-298](#), a report to the Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

General aviation accounts for three-quarters of U.S. air traffic, from small propeller planes to large jets, operating among nearly 19,000 airports. While most security operations are left to private airport operators, the Transportation Security Administration (TSA), part of the Department of Homeland Security (DHS), provides guidance on threats and vulnerabilities. In 2004, TSA issued suggested security enhancements that airports could implement voluntarily. Unlike commercial airports, in most cases general aviation airports are not required to implement specific security measures. GAO was asked to perform onsite assessments at selected airports with general aviation operations to determine what physical security measures they have to prevent unauthorized access.

With advance notice, GAO investigators overtly visited a nonrepresentative selection of 13 airports, based on TSA-determined risk factors. Three of the airports also serve commercial aviation and are therefore subject to TSA security regulations. Using TSA's voluntary recommendations and GAO investigators' security expertise, GAO determined whether certain security measures were in place. GAO also requested documentation of incidents of unauthorized access. Results of GAO's assessments cannot be projected to all general aviation airports and are not meant to imply that the airports failed to implement required security measures.

View [GAO-11-298](#) or key components. For more information, contact Richard J. Hillman at (202) 512-6722 or HillmanR@gao.gov.

May 2011

GENERAL AVIATION

Security Assessments at Selected Airports

What GAO Found

The 13 airports GAO visited had multiple security measures in place to protect against unauthorized access, although the specific measures and potential vulnerabilities varied across the airports. The 3 airports also supporting commercial aviation had generally implemented all the security measures GAO assessed, whereas GAO identified potential vulnerabilities at most of the 10 general aviation airports that could allow unauthorized access to aircraft or airport grounds, facilities, or equipment. For example, 12 of the 13 airports had perimeter fencing or natural barriers as suggested by TSA; but at 6 of the airports fencing was partially bordered by bushes or trees or located next to a parking lot, which can obstruct surveillance or allow someone to scale or topple the fence. GAO found that none of the 10 general aviation airports had lighting along their perimeters. Perimeter lighting provides both a real and psychological deterrent, and allows security personnel to maintain visual assessment during darkness. However, officials at several airports stated that neighborhood street lights provided perimeter lighting, and all 13 airports had lighting around their hangars. The 10 general aviation airports' use of intrusion monitoring varied, with closed-circuit TV (CCTV) cameras and onsite law enforcement being more prevalent than an intrusion detection system, which can consist of multiple monitors including building alarms and CCTV. TSA guidance states that such systems can reduce or replace the need for physical security personnel to patrol an entire facility or perimeter.

Selected Security Measures in Place at 13 Airports

Security measure	General aviation airports (10)			Commercial and general aviation airports (3)		
	Yes	Partial	No	Yes	Partial	No
Perimeter fencing or natural barrier	4	5	1	2	1	0
Perimeter lighting	0	0	10	3	0	0
Lighting around hangars	10	0	0	3	0	0
CCTV cameras	6	3	1	3	0	0
On-site law enforcement or security	4	3	3	3	0	0
Intrusion detection system	0	1	9	3	0	0

Source: GAO.

According to airport officials, several incidents of unauthorized access have occurred within approximately the past 10 years at three of the airports, though they were unable to provide documentation in all cases. Three incidents did not involve access to aircraft, but rather to airport grounds. In separate incidents, two airplanes were stolen or taken from one airport but later recovered. Airport officials informed GAO that they took corrective actions in response to these incidents as appropriate.

DHS generally concurred with GAO's findings and indicated that TSA will work in partnership with the general aviation community to address vulnerabilities. DHS also noted that a lack of funding will be a challenge for most airports. GAO shared its findings with officials at the 13 airports it visited and incorporated their comments as appropriate.

Contents

Letter		1
	Background	4
	Security Measures and Potential Vulnerabilities Identified at Selected Airports	7
	Incidents of Unauthorized Access	16
	Agency Comments and Our Evaluation	17
Appendix I	Scope and Methodology	20
Appendix II	General Aviation Security Measures	23
Appendix III	Comments from the Department of Homeland Security	26
Appendix IV	GAO Contact and Staff Acknowledgments	28
Table		
	Table 1: Security Measures at General Aviation Airports	24
Figures		
	Figure 1: Security Measures in Place at Selected Airports	8
	Figure 2: At Airport without Perimeter Fencing, GAO Investigators Accessing Airport Runway by Car and Approaching Jet Aircraft	10
	Figure 3: Photo of Jet Aircraft Taken from GAO Investigators' Car	11
	Figure 4: Perimeter Fencing Located Next to Trees	12
	Figure 5: Perimeter Fencing Located Next to a Parking Lot	13

Abbreviations

CCTV	closed-circuit television
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
IRS	Internal Revenue Service
TSA	Transportation Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

May 20, 2011

The Honorable John D. Rockefeller IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

General aviation encompasses all civil aviation except scheduled passenger and cargo operations, excludes military flights, and accounts for three-quarters of U.S. air traffic, operating among more than 19,000 airports.¹ This air traffic ranges from small propeller planes flying from private runways to large jets based at major airports. According to the National Air Transportation Association, the general aviation industry contributes about \$150 billion a year to the U.S. economy and employs more than 1.3 million people. Because of the size and diversity of the general aviation industry, as well as the competing needs of commercial aviation, the Transportation Security Administration (TSA), the agency responsible for civil aviation security in the United States, has left most responsibility for security to airport operators, though it does provide guidance on threats and vulnerabilities and imposes regulatory requirements in some cases.²

The damage that can be caused by even small general aviation aircraft was demonstrated by the February 2010 crash of a single-engine plane into an Internal Revenue Service (IRS) building in Austin, Texas.³ Larger aircraft,

¹A general aviation airport is any area of land or water used or intended for use by an aircraft to land or take off, including any buildings or facilities therein, but generally does not include airports subject to security requirements under 49 C.F.R. part 1542, such as airports with scheduled passenger (i.e., commercial) operations. Some airports support both scheduled and general aviation operations. The range of general aviation flight operations encompasses personal/family transportation, power line inspection and repair, pipeline patrol, training, transporting medical supplies, emergency services, rescue operations, wildlife and land surveys, traffic reporting, agricultural aviation, firefighting, and law enforcement.

²A state government can also impose requirements on general aviation operations within its jurisdiction.

³The crash killed the pilot and one IRS employee and injured several other IRS employees. The incident was unrelated to unauthorized access to a general aviation airport.

such as midsized and larger business jets, could cause catastrophic damage to structures and pose a greater risk if they are located near major metropolitan areas. Preventing unauthorized access to general aviation airports and aircraft may help mitigate some security risks.

In response to your interest in the security risks posed by unauthorized individuals gaining access to airports with general aviation operations, we performed on-site assessments at selected airports with general aviation operations to determine what physical security measures they have to prevent unauthorized access. To do so, we identified a nonrepresentative selection of 13 airports that exhibit at least two of the following characteristics that potentially affect an airport's security posture under voluntary TSA guidelines:⁴ (1) airport is a public use airport,⁵ (2) airport location is within 30 nautical miles of a mass population center of at least 1 million people,⁶ (3) based aircraft over 12,500 pounds are located at the airport,⁷ (4) airport has at least one runway with a length of at least 5,000 feet, and (5) over 50,000 annual aircraft operations—takeoffs and landings—occur at the airport. We selected airports from a variety of geographic locations and that represented a range in the number of annual aircraft operations.⁸ Our selection of airports also includes three airports

⁴These characteristics were adapted, in part, from airport characteristics included in TSA's 2004 *Security Guidelines for General Aviation Airports* as components in the measurement tool for airport operators to determine their potential security risk. As discussed in further detail later in this report, the security measures suggested by TSA in the guidelines are entirely voluntary and are not enforceable requirements. See Transportation Security Administration, *Security Guidelines for General Aviation Airports*, Information Publication A-001 (May 2004).

⁵Public use airports are open to the general public, whereas private use airports are intended for use by the owner or for use by the owner and other persons authorized by the owner.

⁶In its 2004 security guidelines, TSA defines a mass population area as an area with a total metropolitan population of at least 100,000 people. For our purposes, we focused on metropolitan areas with populations of at least 1 million people.

⁷Based aircraft are those that are operational and typically based at the airport in question for a majority of the year. An aircraft weighing 12,500 pounds or more is generally equipped with twin turboprop or turbojet engines.

⁸As mentioned above, we attempted to visit airports with more than 50,000 annual aircraft operations. Two of the 13 airports we visited had fewer than 50,000 aircraft operations—both of these airports fall under TSA security requirements because they offer commercial operations.

with both commercial and general aviation operations⁹ that operate under TSA security requirements.¹⁰

With advance notice, we visited all 13 airports and assessed each airport's security measures against TSA's voluntary security guidelines and other criteria based on our expertise in performing security assessments and industry guidance. In addition, we interviewed airport management and other officials; obtained photographic evidence of security measures; requested documentation related to any specific incidents of unauthorized access at each airport; and attempted to obtain information on each airport's procedures, if any, for screening passengers, their carry-on items, and packages or cargo.¹¹

We focused on physical security measures implemented by airports and related to outer airport perimeter security and curbside-to-planeside security.¹² We did not test the effectiveness of the security, nor did we assess measures not directly related to physical security, such as pilot background checks or other intelligence-gathering activities. Although we focused on measures implemented by airports and therefore under direct control of airport management, we gave partial credit when individual aircraft or facility operators, owners, or tenants were responsible for implementing certain security measures.

The results of our assessments are meant to illustrate the variation in physical security conditions at the selected airports. Since TSA does not require the implementation of security measures for airports with only general aviation operations, our assessments are not meant to imply that any of the 13 airports we visited have failed to implement required security measures. Moreover, fixed-base operators at these 13 airports may have security measures in place to prevent unauthorized access that we did not

⁹TSA considers commercial service airports to be those subject to security requirements under 49 C.F.R. part 1542.

¹⁰As discussed later in this report, some general aviation airports fall under TSA security requirements, typically related to an airport's location, size of aircraft, and other factors.

¹¹As discussed later in this report, we did not receive documented security procedures or documentation on incidents of unauthorized access from every airport we visited.

¹²Physical security is just one aspect of overall security provisions. For the purposes of this report, we defined physical security as the combination of operational and security equipment, personnel, and procedures used to prevent unauthorized individuals from gaining access to aircraft or airport facilities and grounds.

observe during our visits.¹³ We generally did not attempt to interview officials from individual operators and we did not examine individual state laws, regulations, or other requirements applicable to general aviation operations.¹⁴ We acknowledge that the specific security measures we focused on are not the only security measures that could prevent unauthorized access. The results of our assessments cannot be projected to all airports with general aviation operations nationwide. We provided officials from all 13 airports an opportunity to comment on our findings as they related to their specific airports. We incorporated their technical comments into our report as appropriate.

We conducted work for this engagement from April 2010 to May 2011 in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency. Additional information about our scope and methodology is provided in appendix I.

Background

General aviation encompasses all civil aviation except scheduled passenger and cargo operations (i.e., commercial) and excludes military operations. It includes air medical-ambulance operations, flight schools, corporate aviation, and privately owned aircraft. Altogether, more than 200,000 aircraft—from small aircraft with minimal payload capacities to business jets and large jets typically used by commercial airlines, such as the Boeing 747—operate at more than 19,000 facilities, including heliports. The sole common characteristic of general aviation operations is that flights are on demand rather than routinely scheduled. General aviation operations take place at more than 5,000 public use airports, almost all of which serve general aviation exclusively. However, general aviation operations may also take place alongside scheduled airline operations at larger commercial airports.

TSA, part of the Department of Homeland Security (DHS), is the primary agency responsible for civil aviation security, which includes general aviation operations.¹⁵ TSA provides the general aviation community with

¹³Fixed-base operators provide a variety of services to pilots, such as flight training, aircraft rental, fueling, maintenance, parking, and the sale of pilot supplies.

¹⁴As discussed later in this report, in some cases airport officials informed us of a state law that affected security measures at their airports.

¹⁵The Federal Aviation Administration also oversees general aviation operations, primarily related to safety—overseeing all aircraft manufacturing, operation, and maintenance; certifying pilots and airports; and regulating air traffic.

guidance on threats and vulnerabilities, and enforces regulatory requirements for specific airports with general aviation operations. However, because of competing needs for commercial aviation security funding and the vastness and diversity of the general aviation network, the bulk of the responsibility for assessing and enhancing security at the general aviation airports falls on airport operators.

In 2004, TSA issued voluntary *Security Guidelines for General Aviation Airports*.¹⁶ These guidelines are intended to provide general aviation airport owners, operators, and users with recommendations for security concepts, technology, and enhancements. In addition, airport operators are encouraged to perform a self-administered risk assessment of their airports based on a measurement tool provided by TSA. TSA recommends that general aviation airports use this tool to determine what security enhancements may be most appropriate to make given the airport's location, number of based aircraft, runway length, and number of annual operations. Based on the results of these self-assessments, the operators can decide whether to implement the appropriate countermeasures suggested, such as fencing; perimeter controls; locks on aircraft, hangars, or both; closed-circuit television (CCTV); lighting; access control systems; and other security features.

In addition to issuing suggested security guidelines, TSA has implemented security requirements that are typically related to an airport's location and size of aircraft. For example, pilots flying to and from general aviation airports within Washington, D.C., airspace must follow security measures including background checks and adherence to specific security procedures. For general aviation flights to and from Ronald Reagan Washington National Airport, TSA officials also inspect crew members and passengers, including performing background checks, and their baggage. In addition, TSA requires private charter services using aircraft that either

¹⁶The Transportation Security Administration developed *Security Guidelines for General Aviation Airports* based on a 2003 report from the Aviation Security Advisory Committee Working Group on General Aviation Airports Security. Working group participants consisted of general aviation industry associations, airport operators, and state and federal government representatives, and was formed to develop guidelines for security enhancements at privately and publicly owned and operated general aviation landing facilities. (For more information, see Transportation Security Administration *Report of the Aviation Security Advisory Committee Working Group on General Aviation Airports Security* (Washington, D.C., Oct. 1, 2003). In November 2010, TSA informed us that the working group would soon reconvene to determine whether and how the general aviation security guidelines should be updated.

(1) have a maximum takeoff weight greater than 100,309 pounds (45,500 kilograms) or (2) have 61 or more passenger seats to implement a security program that includes passenger screening through metal detection devices, X-ray screening for carry-on and checked baggage, and hiring a certified passenger and baggage screening workforce.¹⁷ Individual operators are generally responsible for conducting these requirements rather than airport officials.

In addition, TSA encourages the general aviation community and the public to be vigilant about general aviation security by suggesting specific security awareness and measures for reporting suspicious activity and securing aircraft and aircraft facilities. Examples include

- aircraft with unusual modifications or activity;
- pilots appearing to be under the control of others;
- unfamiliar persons loitering around the field;
- suspicious aircraft lease or rental requests;
- anyone making threats; and
- unusual, suspicious activities or circumstances.

The TSA program also advises aircraft operators to (1) always keep their aircraft locked, (2) refrain from leaving keys in unattended aircraft, (3) use secondary locks or aircraft disablers, and (4) lock hangars when they are unattended.

The Implementing Recommendations of the 9/11 Commission Act of 2007 requires TSA to develop a standardized threat and vulnerability assessment program for general aviation airports and to implement a program to perform such assessments on a risk-managed basis at general aviation airports.¹⁸ From January through April 2010, TSA invited approximately 3,000 general aviation airport operators to complete its online General Aviation Airport Vulnerability Assessment Survey. The survey was intended to highlight the security conditions and vulnerabilities of the general aviation community. According to TSA, the results of the survey were calculated to discover the general strengths and

¹⁷TSA requires that aircraft meeting certain characteristics (based, for example, on the size of the aircraft and whether it is scheduled or chartered) implement security programs pursuant to 49 C.F.R. part 1544. Most aircraft weighing greater than 12,500 pounds are subject to the requirements of a security program. See 49 C.F.R. § 1544.101.

¹⁸See Pub. L. No. 110-53 § 1617, 121 Stat. 266, 488 (Aug. 3, 2007) (codified at 49 U.S.C. § 44901(k)(1)).

weaknesses in the general aviation community, and to show an overall picture of general aviation security measures at a national level and by regions. In addition, TSA stated that the survey results may be used to show a need to develop grants or other means of funding to improve general aviation security measures.¹⁹

Security Measures and Potential Vulnerabilities Identified at Selected Airports

The 13 airports we visited had multiple security measures in place to protect against unauthorized access. The 3 airports that handle commercial flights in addition to general aviation flights (airports 11, 12, and 13 in figure 1) had implemented nearly all of the security measures we assessed. These 3 airports are required to follow TSA regulations because of their commercial flights.²⁰ However, we identified potential vulnerabilities at the 10 general aviation airports that could allow unauthorized access to aircraft or airport grounds, facilities, or equipment. These vulnerabilities include security measures discussed specifically in TSA's 2004 Security Guidelines for General Aviation Airports, which offered suggestions for general aviation airports to voluntarily enhance their security.

Security measures varied across the airports we visited, as well as by the type of security measure. Of the 10 general aviation airports, nearly all had in place or partially in place the following security measures: perimeter fencing or natural barriers, lighting around hangars, aircraft and hangars locked and secured, and CCTV cameras in areas related to unauthorized access. None of the 10 general aviation airports had perimeter lighting in place, and only 1 of the general aviation airports had an intrusion detection system, as discussed below. Figure 1 shows the security measures we observed during our on-site assessments at 13 selected airports.

¹⁹The results of TSA's General Aviation Airport Vulnerability Assessment Survey are considered Sensitive Security Information and are therefore not discussed in this report.

²⁰As mentioned above, commercial service airports are subject to security requirements under 49 C.F.R. part 1542.

Figure 1: Security Measures in Place at Selected Airports

Security measure	Airport												
	General aviation										Commercial/general aviation		
	1	2	3	4	5	6	7	8	9	10	11	12	13
Perimeter fencing/natural barrier	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Controls at designated access points	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
Lighting around perimeter	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
Lighting at designated access points	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓
Lighting around hangars	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hangars locked and secured	✓	✓ _a	✓ _a	✓	✓	✓ _a	✓ _a	✓ _a	✓ _a	✓ _a	✓	✓	✓
Aircraft locked and secured	✓	✓	✓ _a	✓	✓	✓ _a	✓	✓	✓ _a	✓ _a	✓	✓	✓
On-site law enforcement or security	✗	✗	✓	✓	✓	✓	✗	✓ _a	✓	✓	✓	✓	✓
Transient pilot sign-in/sign-out procedures	✗	✓	✓	✓ _a	✓ _a	✗	✓	✗	✓	✗	✓ _a	✓	N/A ^b
Intrusion detection system	✗	✗	✗	✗	✗	✗	✗	✗	✓ _a	✗	✓	✓	✓
CCTV cameras in areas related to unauthorized access	✓	✓	✓	✓ _a	✓	✗	✓	✓	✓ _a	✓	✓	✓	✓
Passenger and baggage screening ^c	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓
Package and cargo screening ^c	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
Back-up generator or power supply	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

✓ Security measure partially in place at the time of our visit

✓ Security measure in place at the time of our visit

✗ Security measure not in place at the time of our visit

Source: GAO.

Notes: Airports 1 through 10 serve general aviation operations, and the security measures suggested by TSA in the Security Guidelines for General Aviation Airports are entirely voluntary and are not enforceable requirements. Airports 11, 12, and 13 serve a combination of commercial and general aviation traffic and are therefore subject to TSA security requirements. We selected the security measures listed above based on our expertise in performing security assessments, a review of security features described in TSA's 2004 *Security Guidelines for General Aviation Airports*, and a review of industry guidance.

^aWe gave partial credit when individual aircraft or facility operators, owners, or tenants were responsible for implementing certain security measures.

^bOnly approved aircraft can access this airport.

^cTSA's suggested guidelines do not discuss physical screening of passengers and their baggage, or of packages and cargo. We included these security measures based on our experience in conducting physical security reviews.

In their technical comments, officials from some airports mentioned security measures that were implemented after we conducted our assessments or that we did not observe in place during our assessments; as such, we were unable to verify that these security measures are in place at the airports in question. For example, an official from airport 1 informed us that the airport has implemented sign-in and sign-out procedures for tracking transient pilots. In addition, an official from airport 9 stated that law enforcement officers provide training on aircraft and hangar security to operators and tenants at the airport.

Fencing. All but one airport had complete or partial perimeter fencing or was protected in part by a natural barrier, such as a body of water. TSA's guidelines suggest that fencing, natural barriers, or other physical barriers can be used to deter and delay the access of unauthorized persons onto sensitive areas of airports—such as terminal areas, aircraft storage, and maintenance areas—and also designed to be a visual and psychological deterrent as well as a physical barrier. One airport had no perimeter fencing in place. While we did not seek to systematically test the effectiveness of security measures in place at all the airports we visited, at this airport our investigators were able to freely drive onto the runway and bring their car next to a jet aircraft. They were not stopped or approached by any airport security, management, or personnel or other individuals while they approached and drove around near the aircraft. According to an official from this airport, it is one of many open field airports located in the United States. He added that pilot vigilance plays a key role in the airport's security, as pilots are responsible for maintaining awareness of suspicious individuals on airport grounds. Figures 2 and 3 show our investigators driving their car onto the runway of this airport and approaching the jet aircraft mentioned above.

Figure 2: At Airport without Perimeter Fencing, GAO Investigators Accessing Airport Runway by Car and Approaching Jet Aircraft



Source: GAO.

Figure 3: Photo of Jet Aircraft Taken from GAO Investigators' Car



Source: GAO.

Although 12 of the 13 airports had full or partial perimeter fencing, or other barriers in place, the fencing at 6 airports was partially bordered by bushes or trees, partially obstructed from view, or located next to a parking lot. TSA's suggested guidelines caution that such factors may limit the effectiveness of perimeter fencing. For example, bushes or other growth can obstruct surveillance of the surrounding areas, and a parking lot may enable someone to use a vehicle to crash through the fence. According to TSA's suggested security guidelines, such incidents have occurred.²¹ Figures 4 and 5 show perimeter fencing located next to trees or a parking lot.

²¹The TSA suggested security guidelines do not specify at what airports these incidents occurred.

Figure 4: Perimeter Fencing Located Next to Trees



Source: GAO.

Figure 5: Perimeter Fencing Located Next to a Parking Lot



Source: GAO.

Lighting. All 13 airports we visited had lighting around their hangars, and all but 3 airports had lighting at designated access points. Ten of the airports we visited—the 10 airports that handle general aviation but not commercial aviation—did not have lighting along their outer perimeters.²² TSA’s suggested guidelines note the effectiveness of lighting in deterring and detecting individuals seeking unauthorized access to airports, but caution that such lighting should not interfere with aircraft operations. The three airports we visited that did have perimeter lighting in place serve a combination of commercial and general aviation traffic. Perimeter lighting provides both a real and psychological deterrent, and allows security personnel to maintain visual-assessment capability during darkness. At several airports we visited, airport managers or other officials stated that streetlights in the neighborhoods surrounding their airports—

²²We did not perform our assessments at night. However, we observed whether lighting systems were in place during our daytime visits.

lights that are not operated or controlled by airport management—provided lighting of the perimeter.

Secured aircraft. All 13 airports we visited had measures at least partially in place so that aircraft and hangars were locked and secured. The 3 airports that serve a combination of commercial and general aviation traffic all had these measures in place. At several general aviation airports, we found that keeping aircraft (4 of 10), hangars (7 of 10), or both locked and secured was the responsibility of individual aircraft or facility operators, owners, or tenants rather than airport management. Two of the airports we visited are located in New Jersey; at these airports, officials informed us that state law requires all aircraft to be secured through the use of two locks.²³ TSA's suggested guidelines note that securing aircraft is the most basic method of enhancing airport security, and that employing multiple methods of securing aircraft makes it more difficult for unauthorized individuals to gain access to aircraft.

On-site security. While most of the airports we visited had on-site law enforcement or other security—such as private security guards—in place, several airports either had no on-site security at all or had on-site security present only during certain times of day, usually in the late evening and early morning. However, the three airports we visited that serve a combination of commercial and general aviation traffic all had this measure in place. Officials from several airports we visited stated that law enforcement officers conduct regular patrols of their airports or respond to emergencies within 3 to 5 minutes; however, these law enforcement officers are not on-site at these airports at all times. The presence of on-site security helps to prevent or impede attempts of unauthorized access, and could include inspection of vital perimeter and access points. TSA's guidelines suggest that airports consider having local law enforcement officers regularly or randomly patrol ramps and aircraft hangar areas, potentially with increased patrols during periods of heightened security.

²³The New Jersey Domestic Security Preparedness Task Force Order (March 21, 2003) requires that all aircraft that are parked or stored for more than a 24-hour period at licensed airports or heliports in the state be secured through a combination of two locking mechanisms. These locking mechanisms can include, among other things, locking tie-down cables, locking hangar doors, locking cockpit doors, and propeller chains. The New Jersey Domestic Security Preparedness Act, NJSA App. A:9-64 *et seq.*, authorizes the Domestic Security Preparedness Task Force to order the implementation of such security measures.

Detecting intruders. Nearly all of the airports we visited—12 of 13—had CCTV cameras installed to monitor for unauthorized access; at 2 of these 12 airports, the CCTV cameras were monitored by individual operators. At one airport, the CCTV cameras were aimed at the administration building and other areas, but not at the perimeter or designated access points. Most of the airports we visited (9 of 13) lacked an intrusion detection system, which may consist of building alarms, CCTV monitoring, or both. TSA guidance states that such systems can replace the need for physical security personnel to patrol an entire facility or perimeter. For example, if an intrusion is detected, the system administrator could notify police, airport management, and other officials. The 3 airports that serve a combination of commercial and general aviation traffic all had CCTV cameras and intrusion detection systems in place. At the time of our visit, an official from airport 4 stated that his airport would soon have an intrusion detection system.

Designated access point controls. Eleven of the 13 airports we visited had controls in place or partially in place at designated access points. All 3 airports that serve commercial and general aviation flights had designated access controls in place. TSA's suggested guidelines note that access point controls should be able to differentiate between an authorized and an unauthorized user, and may be the determining factor in the overall effectiveness of perimeter security in the area of the access point. The airport mentioned above without any perimeter fencing effectively has no access point controls, aside from gates being closed overnight, as was demonstrated when our investigators drove onto the runway unchallenged. An official from this airport informed us that there are gates at the main access points, which are shut when security personnel are on-site from 10:00 p.m. to 6:00 a.m. Another airport had access gates, but they open for all visitors through the use of motion detectors. According to an official from this airport, the motion-controlled access gates allow for individuals to access the airport while keeping wildlife out. At a third airport, there were vehicle access controls that required a code to enter the airport, but there were no pedestrian access controls to prevent individuals from entering onto the ramp area of the airport. An official from this airport told us that individual operators are primarily responsible for controlling those access points. Effective access controls at dedicated vehicle and pedestrian access points help to detect threats and to reduce the possibility that unauthorized individuals will gain access to airports or aircraft.

Screening. Most of the airports we visited did not implement physical screening of passengers and their baggage (8 of 13) or of packages and

cargo (11 of 13) on general aviation flights.²⁴ However, officials at multiple airports told us that pilots typically are familiar with their passengers and may escort them to the aircraft.²⁵ TSA's suggested guidelines related to passengers on general aviation flights state that prior to boarding, the pilot in command should ensure that the identity of all occupants is verified, all occupants are aboard at the invitation of the owner or operator, and all baggage and cargo is known to the occupants. Further, TSA notes that passengers on general aviation flights are generally better known to airport personnel and aircraft operators than most passengers on commercial flights. Two of the 3 airports providing combined commercial and general aviation services implement screening of passengers and their baggage and of cargo and packages. At the third airport, although passenger and baggage screening is conducted, airport officials stated that because they do not perform significant handling of cargo and packages, they do not screen these items.

Incidents of Unauthorized Access

According to airport officials, several incidents of unauthorized access have occurred within approximately the past 10 years at three of the airports we visited. One airport provided documentation detailing two incidents. According to a local police report supplied by airport management and information provided by an airport official, in June 2002 an airline security guard observed a suspicious individual outside the airport's perimeter, near a hangar being constructed. When airport security personnel spotted the individual, he jumped over the perimeter fence onto the airport grounds, and fled into a wooded area covering parts of the perimeter. Local police were called but could not locate the individual after an extensive search. In a 2004 incident, an intoxicated man drove his car onto airport grounds and down a taxiway at high speeds before airport authorities and law enforcement officials apprehended him. While the airport had vehicle access controls, the driver circumvented the controls by following closely behind an authorized vehicle that entered the airport through a gate. Neither of these incidents involved unauthorized individuals accessing aircraft. According to an official from this airport,

²⁴TSA's suggested guidelines do not discuss physical screening of passengers and their baggage or of packages and cargo—such as pat-downs or X-ray machines—but our investigators included this security measure in their on-site assessments based on their experience with conducting physical security reviews.

²⁵During our visits, we did not attempt to verify that pilots at the airports were familiar with passengers.

corrective measures were put in place after each incident. The 2002 incident assisted airport management in developing new security procedures and policies, and the 2004 incident resulted in security training related to vehicle access point controls, among other improvements.

Officials from two other airports described incidents of unauthorized access but did not provide documentation. One airport had two incidents in which aircraft were stolen or removed from the airport without approval: one aircraft was flown to another city in the same state by a teen who knew the combination to the locked hangar in which the aircraft was stored, and the second aircraft was recovered in Mexico. According to an official from this airport, no corrective actions were taken in response to the incident with the teen because he was well known to the aircraft owner and had actually received the combination to the lock from the aircraft owner. The airport also did not implement any corrective actions in response to the incident in which a stolen aircraft was flown to Mexico. However, the airport official stated that the absence of additional aircraft thefts since this incident demonstrates the effectiveness of the airport's existing security measures. At a second airport, unauthorized individuals drove two Corvettes onto the taxiway after obtaining the security code for the vehicle access gate. An official from this airport informed us that the airport requested that local police conduct more frequent patrols in response to this incident.

Officials from 7 of the 13 airports indicated that there were no incidents of unauthorized access at their airports within the past 10 years. We did not receive information about incidents of unauthorized access from officials at the 3 airports with both commercial and general aviation operations. We did not pursue this inquiry because it was not our primary objective.

Agency Comments and Our Evaluation

We met with TSA officials in January 2011 to brief them on the results of our assessments. These officials generally agreed with our findings. According to TSA officials, improvements in general aviation security as a result of TSA's vulnerability assessment surveys will need to be narrowly focused on security measures that can be implemented at a large number of airports yet still prove effective, given the limited resources that may be made available.

In written comments on our report, DHS generally concurred with the overall content and results of our report and indicated that TSA will work in partnership with the general aviation community to support their efforts to address the issues we identified. However, DHS noted TSA security

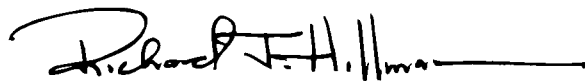
requirements that are not discussed in the Background section of our report. Specifically, TSA requires certain operators of aircraft weighing over 12,500 pounds maximum takeoff weight, based on the type of operation, to adopt a security program and perform security measures, such as checking passenger names against the No-Fly and Selectee Lists, designating security coordinators, and having crewmembers undergo security threat assessments. While our report focused on the physical security measures in place at the specific airports we visited and was not intended to include a comprehensive discussion of all TSA general aviation security initiatives, we acknowledge that TSA has additional security initiatives in place beyond those discussed in our report. DHS also stated that TSA is in the process of issuing a rulemaking for additional security requirements for large general aviation aircraft. According to DHS, TSA expects the release of this rulemaking to further enhance aviation security and codify many of the best practices already implemented by the general aviation industry. In addition, DHS stated that while most airports would readily implement the security measures recommended by TSA, they are unable to put additional security measures in place primarily because of a lack of funding. DHS comments are reprinted in appendix III.

As mentioned above, we provided officials from all 13 airports an opportunity to comment on our findings as they related to their specific airports. As appropriate, we incorporated their technical comments into our report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Homeland Security, the Assistant Secretary of the Transportation Security Administration, selected congressional committees, and other interested parties. The report also will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-6722 or HillmanR@gao.gov. Contact points for our

Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are provided in appendix IV.

A handwritten signature in black ink, reading "Richard J. Hillman", followed by a horizontal line.

Richard J. Hillman
Managing Director
Forensic Audits and Investigative Service

Appendix I: Scope and Methodology

To determine what physical security measures selected airports with general aviation operations have to prevent unauthorized access, we performed on-site assessments at a nonrepresentative selection of 13 airports that exhibit at least two of the following characteristics that potentially affect an airport's security posture under TSA guidelines:¹ (1) airport is a public use airport,² (2) airport location is within 30 nautical miles of a mass population center of at least 1 million people,³ (3) based aircraft over 12,500 pounds are located at the airport,⁴ (4) airport has at least one runway with a length of at least 5,000 feet, and (5) over 50,000 annual aircraft operations—takeoffs and landings—occur at the airport. We selected airports from a variety of geographic locations and in clusters that would allow us to combine multiple on-site assessments on each visit, and that represented a range in the number of annual aircraft operations.⁵ Our selection of airports also includes 3 airports with both commercial and general aviation operations,⁶ and that operate under Transportation Security Administration (TSA) security requirements.⁷

¹These characteristics were adapted from airport characteristics included in the Transportation Security Administration's, *Security Guidelines for General Aviation Airports*, Information Publication A-001 (May 2004), as components in the measurement tool for airport operators to determine their potential security risk.

²Public use airports are open to the general public, whereas private use airports are intended for use by the owner or for use by the owner and other persons authorized by the owner.

³In its 2004 security guidelines, the Transportation Security Administration (TSA) defines a mass population area as an area with a total metropolitan population of at least 100,000 people. For our purposes, we focused on metropolitan areas with populations of at least 1 million people.

⁴Based aircraft include aircraft permanently stationed at an airport by agreement between the aircraft owner and the airport management. An aircraft with a maximum take-off weight of more than 12,500 pounds is generally equipped with twin turboprop or turbojet engines.

⁵As mentioned above, we attempted to visit airports with more than 50,000 annual aircraft operations. Two of the 13 airports we visited had fewer than 50,000 aircraft operations as of November 2010.

⁶TSA considers commercial service airports to be those subject to security requirements under 49 C.F.R. part 1542.

⁷As discussed above, some general aviation operations occur at airports that fall under TSA security requirements.

We traveled to each of the 13 airports we selected and conducted an assessment of the physical security in place to prevent unauthorized access to the airports and aircraft located at the airports.

We assessed each airport's security measures against TSA's 2004 voluntary security guidelines and other criteria based on our expertise in performing security assessments and a review of industry guidance. The security measures we assessed are primarily focused on outer airport perimeter security and curbside-to-planeside security. Physical security is just one aspect of overall security provisions. For the purposes of this report, we defined physical security as the combination of operational and security equipment, personnel, and procedures used to prevent unauthorized individuals from gaining access to aircraft or airport facilities and grounds. We did not test the effectiveness of the security, nor did we assess measures not directly related to physical security, such as pilot background checks or other intelligence-gathering activities. Although we focused on measures implemented by airports and therefore under direct control of airport management, we gave partial credit when individual aircraft or facility operators, owners, or tenants were responsible for implementing certain security measures. At each airport we visited, we interviewed airport management and other officials with knowledge of the security measures. We conducted our on-site assessments with advance notice to airport officials; we did not conduct any undercover testing on this engagement. During our visits, we also obtained photographic evidence of security measures; requested documentation related to any specific incidents of unauthorized access at each airport; and attempted to obtain information on each airport's procedures, if any, for screening passengers, their carry-on items, and packages or cargo by requesting documentation pertaining to their security procedures and measures.

Since TSA does not require the implementation of security measures for airports with only general aviation operations, our assessments are not meant to imply that any of the general aviation airports we visited have failed to implement required security measures. Rather, our assessments are meant to illustrate the variation in security conditions at the selected general aviation airports. We acknowledge that the specific security measures we selected for the purpose of our assessments are not the only security measures that general aviation airports can implement to attempt to prevent unauthorized access. For example, a state government can also impose requirements on general aviation operations within its jurisdiction;

however, the examination of specific state laws, regulations, or other requirements applicable to general aviation operations was not part of our methodology.⁸

Moreover, fixed-base operators at these 13 airports may have additional security measures in place to prevent unauthorized access that we did not observe during our visits.⁹ We generally did not attempt to interview officials from individual operators. We did not test the effectiveness of the security measures that we found in place at the airports we visited. The results of our assessments cannot be projected to all general aviation airports nationwide. We received technical comments from officials representing the 13 airports we visited and incorporated these comments into our report as appropriate.

We conducted work for this engagement from April 2010 to May 2011 in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

⁸As discussed earlier in this report, in some cases airport officials informed us of a state law that affected security measures at their airports.

⁹Fixed-base operators provide a variety of services to pilots, such as flight training, aircraft rental, fueling, maintenance, parking, and the sale of pilot supplies.

Appendix II: General Aviation Security Measures

To perform our security assessment of general aviation airports, we identified 14 key security measures that we determined would help airports to protect against the risk of unauthorized access. The security measures we assessed are primarily focused on outer airport perimeter security and curbside-to-planeside security. We based their selection on our expertise in performing security assessments, a review of security features described in TSA's 2004 *Security Guidelines for General Aviation Airports*,¹ and a review of industry guidance.

A strong physical security system uses layers of security to deter, detect, delay, and deny intruders:

- **Deter.** Physical security measures that deter an intruder are intended to reduce the intruder's perception that an attack will be successful—an armed guard posted at airport access gates, for example.
- **Detect.** Measures that detect an intruder could include video cameras and alarm systems. They could also include roving guard patrols.
- **Delay.** Measures that delay an intruder increase the opportunity for a successful security response. These measures include barriers such as perimeter fences.
- **Deny.** Measures that can deny an intruder include vehicle and pedestrian screening that only permits authorized individuals to access sensitive areas of the airport.

Some security measures serve multiple purposes. For example, a perimeter fence is a basic security feature that can deter, delay, and deny intruders. However, a perimeter fence on its own will not stop a determined intruder. This is why, in practice, layers of security should be integrated in order to provide the strongest protection. Thus, a perimeter fence should be combined with an intrusion detection system that would alert security officials if the perimeter has been breached. A strong system would then tie the intrusion detection alarm to the closed-circuit television (CCTV) network, allowing security officers to immediately identify intruders.

Table 1 shows the security measures we focused on during our assessment work.

¹Transportation Security Administration, *Security Guidelines for General Aviation Airports*.

Table 1: Security Measures at General Aviation Airports

No.	Security measure	Rationale
1	Perimeter fencing/natural barrier	Perimeter fencing surrounding an airport can be used to deter and delay unauthorized individuals from accessing sensitive areas of the airport. Perimeter barriers can also include natural barriers, such as a body of water, and can serve as a visual and psychological deterrent. Areas on both sides of a perimeter fence should be clear—for example, there should be no climbable objects, bushes, trees, or parked vehicles nearby—in order to maintain the effectiveness of the fencing, facilitate surveillance of the perimeter, and reduce unauthorized individuals' ability to find cover near the perimeter.
2	Controls at designated access points	Effective access controls at dedicated pedestrian and vehicle access points help to detect threats and to reduce the possibility that unauthorized individuals will gain access to airports or aircraft.
3	Lighting around perimeter	Lighting around the outer perimeter aids surveillance at night or in other dark conditions, and also enhances the level of psychological deterrent.
4	Lighting at designated access points	Lighting at designated access points increases visibility and helps to protect against unauthorized access at night or in other dark conditions, and also enhances the level of psychological deterrent.
5	Lighting around hangars	Lighting around hangars helps protect against theft, vandalism, and other illegal activity at night or in other dark conditions.
6	Hangars locked and secured	Storing aircraft in locked hangars is an effective way to protect against unauthorized access. Locks provide physiological deterrence and make it more difficult for unauthorized individuals to access aircraft. Locks may also increase the chance of detecting such individuals due to the loss in time and the usual added noise required to bypass a lock.
7	Aircraft locked and secured	Locks provide physiological deterrence and make it more difficult for unauthorized individuals to access aircraft. Locks may also increase the chance of detecting such individuals because of the loss in time and the usual added noise required to bypass a lock.
8	On-site law enforcement or security	The presence of on-site security helps to prevent or impede attempts of unauthorized access, and could include inspection of vital perimeter and access points.
9	Transient pilot sign-in/sign-out procedures	Sign-in/sign-out procedures for transient pilots help to identify nonbased pilots and aircraft using airport facilities.
10	Intrusion detection system	An intrusion detection system can replace the need for personnel to patrol an entire facility or perimeter.
11	CCTV cameras in areas related to unauthorized access	CCTV cameras can be an alternative to perimeter fencing or, together with perimeter fencing, can deter unauthorized individuals from attempting to access airport grounds and facilities. In addition, CCTV cameras may reduce the need for multiple individuals to maintain constant surveillance on all sensitive areas of a facility.
12	Passenger and baggage screening ^a	Passenger and baggage screening can help to prevent unauthorized individuals from accessing aircraft or from bringing prohibited or destructive items onboard aircraft or into sensitive areas of the airport.

Appendix II: General Aviation Security Measures

No.	Security measure	Rationale
13	Package and cargo screening ^a	Package and cargo screening can help to prevent prohibited or destructive items from being brought onboard aircraft or into sensitive areas of the airport.
14	Backup generator or power supply	Backup generators or other power supplies may help to maintain essential security functions at airports if the main power supply is disabled or otherwise compromised.

Sources: GAO and GAO analysis of TSA's *Security Guidelines for General Aviation Airports*.

^aTSA's suggested guidelines do not discuss physical screening of passengers and their baggage or of packages and cargo. We included these security measures based on our experience in conducting physical security reviews.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

April 26, 2011

Mr. Richard J. Hillman
Managing Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Comments to Draft Report, GAO-11-298, "GENERAL AVIATION:
Security Assessments at Selected Airports"

Dear Mr. Hillman:

Thank you for the opportunity to review and comment on draft report GAO-11-298, titled: *General Aviation: Security Assessments at Selected Airports*. The Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) appreciate the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

While DHS concurs with the overall content and results of the report, the Department would like to point out that the report's background discussion of TSA's security requirements omits the general aviation security program. TSA requires certain operators of aircraft over 12,500 pounds maximum takeoff weight, based on the type of operation, to adopt a security program and perform security measures such as checking passenger names against the No Fly and Selectee Lists (which are subsets of the Terrorist Screening Database (TSDB)), designating security coordinators, and having crewmembers undergo security threat assessments.

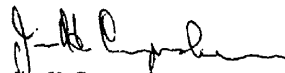
Additionally, TSA is in the process of issuing a rulemaking for large general aviation aircraft. In October 2008, TSA issued a Notice of Proposed Rulemaking for the Large Aircraft Security Program, which would have imposed security requirements on all aircraft over 12,500 pounds maximum takeoff weight. TSA received more than 8,000 public comments and held a series of public hearings and industry comment sessions to solicit further feedback. TSA has taken this feedback under consideration while drafting a Supplemental Notice of Proposed Rulemaking (SNPRM). The SNPRM is currently undergoing review within TSA and DHS, with an anticipated release for public comment later this year. TSA expects the release of this rulemaking to further enhance aviation security and codify many of the best practices already implemented by the general aviation industry.

TSA would also like to note that while most airports would readily implement the security measures recommended by TSA, they are unable to put additional security measures in place primarily because of a lack of funding. TSA does not currently have a grant program to assist airports with funding for security projects, and there are limitations on the use of funding that airports may receive through the Federal Aviation Administration's (FAA's) Airport Improvement Program (AIP) grants. The FAA requires that airports match AIP funding with 10 percent of their own funding. Many airports are unable to raise this portion of the project funding, so are unable to accept the AIP grants to implement measures, such as fencing, that could enhance both safety (FAA's mandate) and security (TSA's mandate).

In conclusion, TSA strongly believes that general aviation airports are complying with recommended security measures to the extent that those measures are practical and effective given the unique conditions at each airport, and to the extent that funding is available for the desired security enhancements. TSA appreciates GAO's work to identify opportunities to enhance security at general aviation airports and will continue to work in partnership with the general aviation community to support their efforts to address the issues identified by GAO. The close working relationship with general aviation stakeholders is a vital component of TSA's mission to secure the Nation's transportation systems.

Thank you for the opportunity to comment on this Draft Report. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Richard J. Hillman, (202) 512-6722 or HillmanR@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff members made significant contributions to this report: Gregory D. Kutz, Director; Cindy Brown-Barnes, John Cooney, and Andy O'Connell, Assistant Directors; John R. Ahern, Christopher W. Backley; Betsy Isom; Maria Kabiling; Barbara Lewis; Olivia Lopez; Steve Martin; Flavio J. Martinez; George Ogilvie; Barry Shillito; and Tim Walker.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

